

AMENDMENT

In the claims:

1-64 (Canceled)

65. (New) A security device comprising at least one magnetic element, wherein said at least one magnetic element is responsive to an applied magnetic field to provide a characteristic response, wherein said at least one magnetic element is made from a material that comprises structural defects that cause brittle mode switching in which the growth of a single magnetic domain dominates the change in magnetisation of a respective magnetic element.

66. (New) The security device of Claim 65, wherein said at least one magnetic element is supported by a substrate.

67. (New) The security device of Claim 66, wherein said at least one magnetic element is supported on said substrate.

68. (New) The security device of Claim 65, wherein said at least one magnetic element is responsive to said applied magnetic field to switch the magnetisation or magnetic polarisation of said at least one magnetic element.

69. (New) The security device of Claim 66, wherein said at least one magnetic element is made from a magnetically soft material.

70. (New) The security device of Claim 69, wherein said at least one magnetic element comprises a magnetically soft material selected from one or more of: nickel, iron, cobalt and alloys thereof with each other or silicon, such as nickel iron alloy, cobalt iron alloy, iron silicon alloy or cobalt silicon alloy.

71. (New) The security device of Claim 69, wherein said magnetically soft material is a permalloy material.

72. (New) The security device of Claim 65, wherein said at least one magnetic element is substantially wire-shaped or flattened wire shaped.
73. (New) The security device of Claim 65, wherein said at least one magnetic element is backed by a light reflective layer.
74. (New) The security device of Claim 65, wherein said at least one magnetic element is provided proximal a reduced light reflectivity portion of said security device.
75. (New) The security device of Claim 65, comprising a plurality of said at least one magnetic elements.
76. (New) The security device of Claim 75, wherein said plurality of magnetic elements is arranged to provide a linear pattern.
77. (New) The security device of Claim 75, wherein said plurality of magnetic elements is arranged to provide a two-dimensional pattern.
78. (New) The security device of Claim 76, wherein said pattern encodes an identifier.
79. (New) The security device of Claim 65, further comprising a unique identifier incorporated therewith.
80. (New) The security device of Claim 79, wherein said unique identifier is provided by way of one or more of: an optically readable bar code; one or more optical indicia; a magnetically encoded identifier; and an electronic identifier.
81. (New) The security device of Claim 80, mounted upon a smart-card, wherein said electronic identifier is provided by a smart-card chip provided on said smart-card.
82. (New) The security device of Claim 65, wherein premeasured characteristic response information representing one or more measurable parameters of said characteristic response is stored on said security device.

83. (New) The security device of Claim 82, wherein said premeasured characteristic response information is in encrypted form.
84. (New) A method of manufacturing a security device, comprising:
providing at least one magnetic element comprising structural defects, wherein said at least one magnetic element provides a brittle mode switching characteristic response in response to an applied magnetic field.
85. (New) The method of Claim 84, comprising providing said at least one magnetic element on a substrate.
86. (New) The method of Claim 84, comprising forming said at least one magnetic element using a lift-off or wet etching process.
87. (New) The method of Claim 84, comprising forming said at least one magnetic element using an ion beam etching process.
88. (New) The method of Claim 84, comprising measuring the magnitude(s) of one or more magnetic parameters of said at least one magnetic element.
89. (New) The method of Claim 88, comprising measuring one or more of coercivity and jitter values.
90. (New) The method of Claim 88, comprising using the measured magnitude(s) of said one or more magnetic parameters to represent premeasured characteristic response information.
91. (New) The method of Claim 90, comprising encrypting said premeasured characteristic response information.
92. (New) The method of Claim 90, comprising storing said premeasured characteristic response information in encrypted or unencrypted form on said security device.

93. (New) The method of Claim 90, comprising storing said premeasured characteristic response information in encrypted or unencrypted form in a storage medium remote from said security device.
94. (New) The method of Claim 93, comprising storing said premeasured characteristic response information in encrypted or unencrypted form in a database.
95. (New) The method of Claim 84, further comprising providing said security device with a unique identifier.
96. (New) The method of Claim 95 when dependant upon any one of Claims 27 to 30, comprising storing a representation of said unique identifier in association with said premeasured characteristic response information.
97. (New) A system for reading a security device, comprising:
a magnetic field generation system for applying a magnetic field to a security device;
and
a detection system for measuring one or more parameters representative of a brittle mode switching measured characteristic response of said security device in response to said magnetic field,
wherein said system is operable to compare said one or more parameters representative of a brittle mode switching measured characteristic response to one or more respective parameters of a brittle mode switching premeasured characteristic response to determine whether respective measured and premeasured parameters are substantially equivalent.
98. (New) The system of Claim 97, wherein the magnetic field generation system is operable to apply a time varying magnetic field to a security device.
99. (New) The system of Claim 97, wherein a light beam is used to interrogate said security device.
100. (New) The system of Claim 97, wherein said light beam is a visible or near-infrared beam produced by a laser diode.

101. (New) The system of Claim 97, wherein said parameters represent one or more of coercivity and jitter values.
102. (New) The system of Claim 99, wherein said detection system incorporates magneto-optic Kerr effect detection apparatus for detecting changes induced in said light beam by magnetic elements of said security device.
103. (New) The system of Claim 102, wherein said magneto-optic Kerr effect detection apparatus is configured to operate in transverse mode.
104. (New) The system of Claim 99, further operable to deflect said light beam across the surface of said security device.
105. (New) The system of Claim 99, further operable to read a unique identifier from said security device.
106. (New) The system of Claim 105, wherein said unique identifier is identified by recognising a pattern of magnetic elements supported by said security device.
107. (New) The system of Claim 105, wherein said unique identifier is identified by reading one or more of: an optically readable bar code; one or more optical indicia; a magnetically encoded identifier; and an electronic identifier.
108. (New) The system of Claim 97, further operable to determine said one or more respective parameters of the premeasured characteristic response by reading said one or more parameters from said security device.
109. (New) The system of Claim 97, further operable to determine said one or more respective parameters of the premeasured characteristic response by reading said one or more parameters from a database.
110. (New) The system of Claim 109, wherein said database is remotely located from said detection system.

111. (New) The system of Claim 97, further operable to decrypt premeasured characteristic response information where it is read or provided in encrypted form.
112. (New) A method for reading a security device, comprising:
applying a magnetic field to a security device;
measuring one or more parameters representative of a brittle mode switching measured characteristic response of said security device in response to said magnetic field;
and
comparing said one or more parameters representative of a brittle mode switching measured characteristic response to one or more respective parameter(s) of a brittle mode switching premeasured characteristic response to determine whether respective measured and premeasured parameters are substantially equivalent.
113. (New) The method of Claim 112, comprising applying a time varying magnetic field to a security device.
114. (New) The method of Claim 112, wherein measuring of one or more parameters representative of a measured characteristic response of said security device in response to said magnetic field comprises measuring one or more of coercivity and jitter values.
115. (New) The method of Claim 112, comprising interrogating said security device using a light beam.
116. (New) The method of Claim 112, comprising operating a laser to produce a visible or near-infrared beam.
117. (New) The method of Claim 115, comprising detecting changes induced in said light beam by magnetic elements of said security device using the magneto-optic Kerr effect.
118. (New) The method of Claim 117, comprising using the magneto-optic Kerr effect transverse mode.
119. (New) The method of Claim 115, comprising deflecting said light beam across the surface of said security device.

120. (New) The method of Claim 112, comprising reading a unique identifier from said security device.

121. (New) The method of Claim 120, comprising identifying said unique identifier by recognising a pattern of magnetic elements supported by said security device.

122. (New) The method of Claim 120, comprising identifying said unique identifier by reading one or more of: an optically readable bar code; one or more optical indicia; a magnetically encoded identifier; and an electronic identifier.

123. (New) The method of Claim 112, comprising determining said respective one or more parameters of the premeasured characteristic response by reading said one or more parameters from said security device.

124. (New) The method of Claim 112, comprising determining said one or more respective parameters of the premeasured characteristic response by reading said one or more parameters from a database.

125. (New) The method of Claim 124, comprising accessing a database remotely located from said detection system.

126. (New) The method of Claim 112, further comprising decrypting premeasured characteristic response information where it is read or provided in encrypted form.

127. (New) A product comprising a security device comprising at least one magnetic element, wherein said at least one magnetic element is responsive to an applied magnetic field to provide a characteristic response, wherein said at least one magnetic element is made from a material that comprises structural defects that cause brittle mode switching in which the growth of a single magnetic domain dominates the change in magnetisation of a respective magnetic element.

128. (New) The product of Claim 127, comprising one or more of: a document; a passport; an identity card; a compact disc; a digital versatile disc; a software product; packaging; an item of clothing; an item of footwear; a smart-card; a credit or bank card; a

cosmetic item; an engineering part; an accessory; and any other goods and/or items of commerce, whether manufactured or otherwise.